УДК 368.1

ТЕНДЕНЦИИ КИБЕРСТРАХОВАНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Андрейковец В.И.

Студент Факультета «Мировая экономика и право»

Сибирский государственный университет путей сообщения

Новосибирск, Россия

Железнюк А.Е.

Студент Факультета «Мировая экономика и право»

Сибирский государственный университет путей сообщения

Новосибирск, Россия

Конюкова О.Л.

к.э.н., доцент

Сибирский государственный университет путей сообщения

Новосибирск, Россия

Аннотация: Данная статья посвящена вопросам необходимости киберстрахования в цифровой экономике РФ, рассмотрены его преимущества и этапы. Проведен анализ кибератак в целом на рынке и в разрезе основных участников: физических и юридических лиц. Также рассмотрена структура кибератак во всех отраслях экономики и выявлены наиболее подверженные риску. В статье проведен сравнительный анализ лидирующих компаний, страхующих киберриски в РФ, а также рассмотрена реальная модель киберстрахования на примере «Сбербанк Страхование» и «Додо пицца».

Ключевые слова: страхование, киберстрахование, цифровизация, киберриск, кибератака, страховые риски, информационные системы.

TRENDS IN CYBERINSURANCE IN THE RUSSIAN FEDERATION

Andrejkovets V.I.
Student of the Faculty «World Economy and Law»
Siberian State University of Railways
Novosibirsk, Russia
Zheleznyuk A.E.
Student of the Faculty «World Economy and Law»
Siberian State University of Railways
Novosibirsk, Russia
Konyukova O.L.
Ph.D., Associate Professor
Siberian State University of Railways
Novosibirsk, Russia

Abstract: This article is devoted to the need for cyber insurance in the digital economy of the Russian Federation, its advantages and stages are considered. The analysis of cyberattacks in general in the market and in the context of the main participants: individuals and legal entities was conducted. Also the structure of cyberattacks in all branches of economy has been considered and the most at risk have been identified. The article conducts a comparative analysis of the leading companies that insure cyberrisks in the Russian Federation, and also considers the real model of cyber insurance on the example of «Sberbank Insurance» and «Dodo pizza».

Keywords: insurance, cyber insurance, digitalization, cyberrisk, cyber attack, insurance risks, information systems.

Страхование играет важную роль в экономике, так как оно помогает снижать финансовые риски и обеспечивать стабильность в различных ее

секторах, а также защищает от финансовых потерь, поддерживает экономическую стабильность, содействует инвестициям и предпринимательству, социальному обеспечению. В настоящее время происходит активное развитие IT-технологий, а как следствие возникают новые финансовые риски для общества, так как процесс превращения аналоговых данных в цифровой формат сопряжен с возникновением различных атак, краж и прочих преступлений в сети Интернет.

Под цифровизацией необходимо понимать использование и внедрение новых цифровых технологий, основной целью которых будет являться повышение эффективности и результативности деятельности государственных органов. Это может быть как изменение отдельных процессов, так и что-то большее. Эпоха цифровизации, охватывающая всё большие отрасли, в перспективе затронет все сферы экономии и многие существующие компании [5].

В связи с этим существует необходимость развития сектора страхования, так как процесс цифровизации оказывает существенное воздействие на данную отрасль и выступает основой для перспективного направления - киберстархования, предоставляя необходимую инфраструктуру и инструменты для обработки и передачи данных. Таким образом, киберстрахование - это вид страхования, который предназначен для защиты от потенциальных угроз, связанных с киберпреступностью и киберрисками [1].

Роль киберстрахования в экономике заключается в обеспечении финансовой защиты и минимизации рисков, связанных с кибератаками и другими киберугрозами для компаний и организаций. Киберстрахование помогает предприятиям справиться с потенциальными убытками, связанными с нарушением безопасности данных, нарушением работы информационных систем, кражей личной информации, шантажем и другими киберпреступлениями.

Киберстрахование позволяет компаниям получить компенсацию за ущерб, понесенный в результате кибератаки или другого инцидента безопасности данных. Киберстрахование также может предоставлять услуги по обнаружению и предотвращению киберугроз, а также содействовать восстановлению после инцидента.

Страхование киберрисков впервые появилось в США в 1999 году. В России данный вид страхования предлагается только с октября 2012 года [6].

Рынок киберстрахования является одним из приоритетных направлений развития не только страхования, но и экономики в целом. По данным международных экспертов, по состоянию на 2022 год глобальный рынок страхования киберрисков достигнет 14 млрд долл. США, а к 2025 году он будет составлять уже 20 млрд долл. США [3]. Задача страхования киберрисков состоит в покрытии убытков, возникших в результате успешно реализованных кибератак. Банк России планирует сформировать условия создания института страхования киберрисков, и предоставить расширенный перечень данных внешним пользователям для формирования моделей страхования.

Сегодня на рынке страхования РФ доля киберстрахования крайне мала и составляет чуть более 1%, что является достаточно низким показателем в общей структуре рынка. Существует несколько причин, почему кибератаки растут, а киберстрахование имеет маленькую долю на рынке страхования:

— Сложность оценки риска: из-за сложности прогнозирования и оценки рисков, страховые компании испытывают трудности в разработке политик страхования и определении адекватных тарифов;

— Определение ущерба: компании могут столкнуться с проблемой определения фактических потерь и восстановительных затрат, что затрудняет страховые выплаты;

— Высокая стоимость страхования: киберстрахование является дорогим, особенно для малых и средних предприятий. Высокие ставки премий и

недостаток данных о потенциальной выгоде от страхования могут отпугивать компании от покупки полисов;

— Отсутствие обязательного страхования: В РФ киберстрахование не является обязательным, следовательно, компании не чувствуют необходимости приобретать полисы;

— Недостаток осведомленности: многие компании не полностью осознают риски, связанные с кибератаками, и потенциальную пользу от киберстрахования;

— Недостаточное регулирование: для компаний барьер заключается в том, что в большинстве случаев затраты на страхование киберрисков нельзя отнести к себестоимости предприятия и бизнес не получает налоговые послабления [4].

Таким образом, кибератака – это попытка обойти методы защиты информационной системы недобросовестными членами общества с целью получения несанкционированного доступа к системам и данным, внесения изменения в работу систем, их полной или частичной остановки. Всемирный экономический форум оценивает данный риск как третий по величине с точки зрения вероятности и шестой по степени воздействия среди всех рисков в отчете [2].

Для анализа состояния рынка киберстрахования в РФ необходимо рассмотреть динамику кибератак за период II квартал 2021- II квартал 2023 гг. [3] на основании данных Банка России, представленную на рисунке 1.

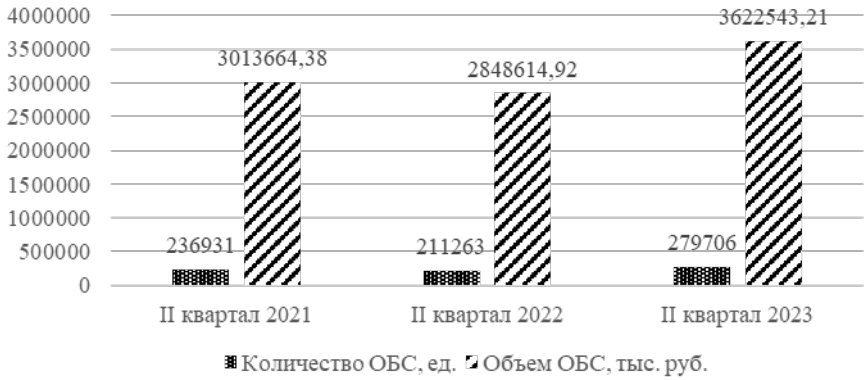

Рисунок 1 – Динамика операций без согласия клиентов (ОБС): общая картина за период II квартал 2021- II квартал 2023 гг.

Источник: составлено автором

Исходя из данных рисунка 1, наблюдается негативная динамика, так как происходит увеличение кибертак на 42 775 ед. или 608 878,83 тыс. руб. Это свидетельствует о том, что ежегодно риски кибератак увеличиваются и спрос на киберстрахование возрастает. Однако, грамотное регулирование во II квартале 2021,2022 и 2023 гг. позволило возместить долю средств (от объема): 7,4%, 5% и 4,6% соответственно. Здесь также наблюдается негативная динамика: при росте кибератак количество страхователей остается на прежнем уровне или незначительно увеличивается и, как следствие, страховую выплату получает небольшой процент пострадавших от атаки лиц. Также следует отметить, что за II квартал 2023 года было предотвращено 6 598 750 операций без согласия клиентов, что является положительным моментом.

Рассмотрим структуру кибератак на рынке киберстрахования в разрезе основных участников: физические и юридические лица за II квартал 2023 г., представленную на рисунке 2.

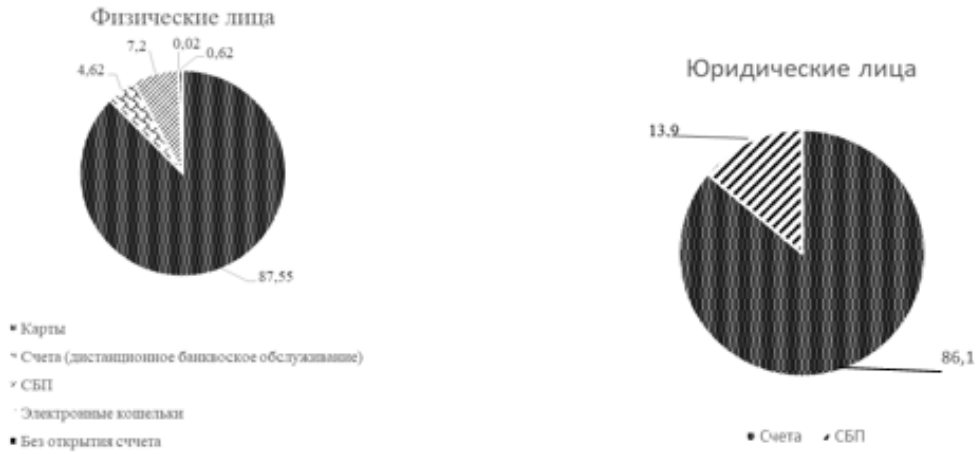

Рисунок 2 – Структура кибератак в разрезе основных участников рынка: физические и юридические лица за II квартал 2023 г., %

Источник: составлено автором

Анализируя данные рисунка 2, можно сделать вывод о том, что кибератакам подвергаются все участники рынка, т.е. и физические и юридические лица. Наибольшая доля кибератак у физических лиц приходится на банковские каты (1 700 972,78 тыс. руб.) и СБП (767 881,33 тыс. руб.). У юридических лиц наиболее подверженными кибератакам являются счета (91 130,39 тыс. руб.). Стоит отметить, что физические лица чаще подвергаются кибератакам из-за их ограниченной осведомленности о кибербезопасности, меньших ресурсов для установки сильных защитных мер, а также из-за большего количества потенциальных целей для злоумышленников.

Киберстрахование обладает рядом преимуществ для всех участников рынка:

— Защита от финансовых потерь: киберстрахование помогает компаниям и частным лицам защититься от финансовых убытков, связанных с киберпреступлениями, включая потерю данных, мошенничество и утрату прибыли;

— Экспертная помощь и восстановление: страховые компании предоставляют поддержку в восстановлении данных и систем после кибератаки;

— Юридическая защита: киберстрахование покрывает расходы на юридическую помощь в случае возникновения правовых вопросов, связанных с киберугрозами;

— Мониторинг и предупреждение: некоторые полисы включают услуги мониторинга кредитных отчетов и оповещения о подозрительной активности, что помогает предотвращать мошенничество;

— Предотвращение репутационных потерь: киберстрахование может помочь компаниям восстановить репутацию и доверие клиентов после кибератаки через эффективное управление кризисной ситуацией и общественными отношениями;

— Снижение риска: защищенные компании могут снизить риск кибератак и повысить доверие клиентов и партнеров, что способствует устойчивости бизнеса.

Страховые риски присутствуют во всех сферах жизни общества, а в следствие развития цифровизации появляется их новый вид – киберриски. Банк России определяет киберриск как риск преднамеренного воздействия работников финансовой организации, третьих лиц, внутренних (в том числе с применением компонентов иностранного производства) и (или) сторонних информационных систем, направленного на несанкционированное получение (хищение), из-менение, удаление данных и иной цифровой информации и (или) структуры данных, параметров и характеристик систем (в том числе программного кода) и режима доступа посредством цифровой инфраструктуры и технологий связи, в том числе путем реализации компьютерных атак [1].

Так как существуют киберриски, то присутствует необходимость их страхования с целью безопасности для бизнеса или отдельного лица. С этой целью осуществляется киберстрахование в различных отраслях, поэтому

необходимо рассмотреть структуру воздействия кибератак на каждую отрасль экономики в отдельности за II квартал 2023 года, представленную на рисунке 3

Рисунок 3 – Структура кибератак в разрезе отраслей экономики за II квартал 2023 г., %

Источник: составлено по данным Банка России [3]

Исходя из данных рисунка 3 наибольшей кибератаке подвергаются предприятия без привязки к отрасли (15%), которые также называются диверсифицированными предприятиями или конгломератами. Эти компании владеют или контролируют бизнес в различных отраслях, таких как финансы, производство, технологии, розничная торговля, например, Samsung, Virgin Group, Siemens. На втором месте по кибератакам находятся госучреждения, обладающие 14% в общей структуре, что происходит по нескольким причинам:

— Государственные учреждения хранят и обрабатывают большое количество ценных данных, таких как персональная информация о гражданах, финансовые данные и государственные секреты;

— Государственные деятели могут пытаться вмешаться в политические процессы или нарушить работу критической инфраструктуры для достижения своих целей;

— Некоторые кибератаки на государственные учреждения могут быть направлены на нанесение ущерба их репутации и доверию общества к правительству.

В настоящее время на российском рынке лидирующие позиции по киберстрахованию занимают такие компании как: «АльфаСтрахование», «АИГ страховая компания», «Зетта страхование», «Сбербанк Страхование». Сравнительная характеристика лидеров рынка, предоставляющих услуги по киберстрахованию представлена в таблице 1.

Таблица 1 – Сравнительная характеристика лидирующих компаний, страхующих киберриски в РФ

Компания	Общая характеристика	Какие риски страхуют
АльфаСтрахование	Предлагает своим клиентам продукт АльфаCyber, который позволяет заключить договор о кибероопасности для всех или некоторых аспектов их бизнеса.	Утрата информации; Хищение интеллектуальной собственности; Неправомерное использование вычислительных ресурсов; Вымогательства; Хищения денежных средств; Нарушение конфиденциальности и разглашение персональных данных; Ущерб деловой репутации.
АИГ страховая компания (AIG)	Разработала программу страхования CyberEdge, которая предлагает широкий и комплексный подход к защите персональных данных на предприятии от утечки или незаконного использования.	Убытки в связи с нарушениями данных; Административное расследование в отношении данных; Расходы на реагирование при нарушении данных; Ответственность за содержание информации; Виртуальное вымогательство; Перерыв в работе сети.
Зетта страхование	Разработала свой продукт по страхованию кибер-рисков Allianz Cyber Protect.	Гражданская ответственность за утрату персональных и финансовых данных клиентов; Убытков, которые несет сам застрахованный по причине простоя, кибервымогательства; Покрытие расходов на расследование инцидентов и

		помощь со стороны специалистов по форензику.
Сбербанк Страхование	Предлагает пять программ страхования. Под страховой защитой находятся программное обеспечение, корпоративная электронная почта, сайты, облачные сервисы и базы данных компаний.	Кибератаки и хакерские атаки; Финансовые мошенничества; Потеря или повреждение данных; Подрыв репутации; Штрафы и санкции.

Исходя из проведенной сравнительной характеристики, представленной в таблице 1 наблюдается значительно широкий перечень услуг по киберстрахованию разными организациями. Безусловно, услуги всех четырех компаний имеют схожую направленность, но каждая из организаций обладает своим уникальным продуктом, например, Сбербанк осуществляет страхование «штрафов и санкций», т.е. в случае утечки информации на организацию могут быть наложены штрафные санкции и «Сбербанк Страхование» покроет все расходы связанные с ними. Страховая копания «Зетта страхование» предлагает своим клиентам возмещение в случае простоя, когда электронный ресурс подвергся кибератаке и деятельность организации временно приостановилась. В зависимости от того, с какой потребностью обращаются в страховую организацию страхователи могут быть предложены различные программы (пакеты) страхования, которые отличаются как в цене, так и перечнем предоставляемых услуг. Стоимость киберстрахования зависит от набора рисков, страховой суммы и франшизы, а также рода деятельности страхователя и результатов оценки рискозащищенности. Процесс киберстрахования включает несколько этапов:

1 этап – страховщик проводит оценку рисков для определения уровня уязвимости и потенциальных угроз для страхуемого. Это может включать анализ систем безопасности, политик и процедур, а также истории предыдущих инцидентов;

2 этап – страховой провайдер и страхователь определяют необходимый уровень покрытия и типы рисков, которые будут включены в страховой полис.

Это может включать защиту от кибератак, ущерба системам и данным, расходов на восстановление и репутационных потерь;

3 этап – после согласования условий страхования и оплаты премии, страхователь и страховщик заключают страховой полис, который является юридическим документом, определяющим права и обязанности сторон;

4 этап – в течение срока действия страхового полиса, страховщик может проводить мониторинг и анализ состояния кибербезопасности страхуемого. Это может включать аудиты, проверки уязвимостей и консультации по улучшению безопасности;

5 этап – в случае кибератаки или нарушения безопасности, страховщик предоставляет поддержку и ресурсы для реагирования на инциденты. Это может включать финансовую компенсацию за ущерб, юридическую помощь и экспертное консультирование.

Таким образом, киберстрахование является неотъемлемой частью в современного цифрового мира, где обеспечение сохранности баз данных является одной из важнейших задач для организаций, так как они в наибольшей степени подвергаются киберугрозам. С этой целью разрабатываются программы по страхованию информационных систем, например, 11 июля 2019 года между «Сбербанк страхование» и «Додо пицца» был заключен договор для страхования их информационных систем и ресурсов от киберрисков. В рамках данного договора были застрахованы: программное обеспечение, корпоративная электронная почта, веб-сайт, «облачный» сервис и базы данных компании «Додо пицца». Договор был заключен по программе MyCyberInsurance Optima, которая предусматривает страхование убытков от перерыва в хозяйственной деятельности и несанкционированного списания денег со счета клиента в результате киберинцидента, а также страхование гражданской ответственности за вред, причиненный третьим лицам в результате кибератаки. Необходимость киберстрахования объяснялось тем, что «Додо пицца» разработала облачную систему управления пиццерией под названием «Додо ИС», которая покрывает

все аспекты их бизнеса, включая заказы клиентов, мобильное приложение и сайт, процессы приготовления пиццы, работу кассы и прием платежей, а также все операционные процессы пиццерии и другие важные функции. Им необходимо, чтобы их информационная система работала без сбоев, поэтому они решили направить средства на её страховую защиту.

Библиографический список:

1. Страхование : учебник и практикум для вузов / И. П. Хоминич [и др.] ; под общей редакцией И. П. Хоминич. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 620 с. — (Высшее образование). — ISBN 978-5-534-17677-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/533525 (дата обращения: 05.10.2023).
2. Войцехович А. В., Адамчук Н. Г. Международный рынок киберстрахования / / Страховое право. 2017. № 4 (77). С. 31—36.
3. Банк России. [Электронный ресурс]. – Режим доступа: – URL: http://www.cbr.ru (Дата обращения: 07.10.2023).
4. Banki.ru. [Электронный ресурс]. – Режим доступа: – URL: https://www.banki.ru/news/daytheme/?id=10935956 (Дата обращения: 09.10.2023)
5. Роль цифровизации в государственном управлении Конюкова О.Л., Летунов С.А. Global and Regional Research. 2019. Т. 1. № 1. С. 74-79.
6. Конюкова О.Л., Рагозин Н.А. Применение киберстрахования в современных условиях развития экономики //Вектор экономики. 2020. №5 (47). С. 71

Оригинальность – 76%